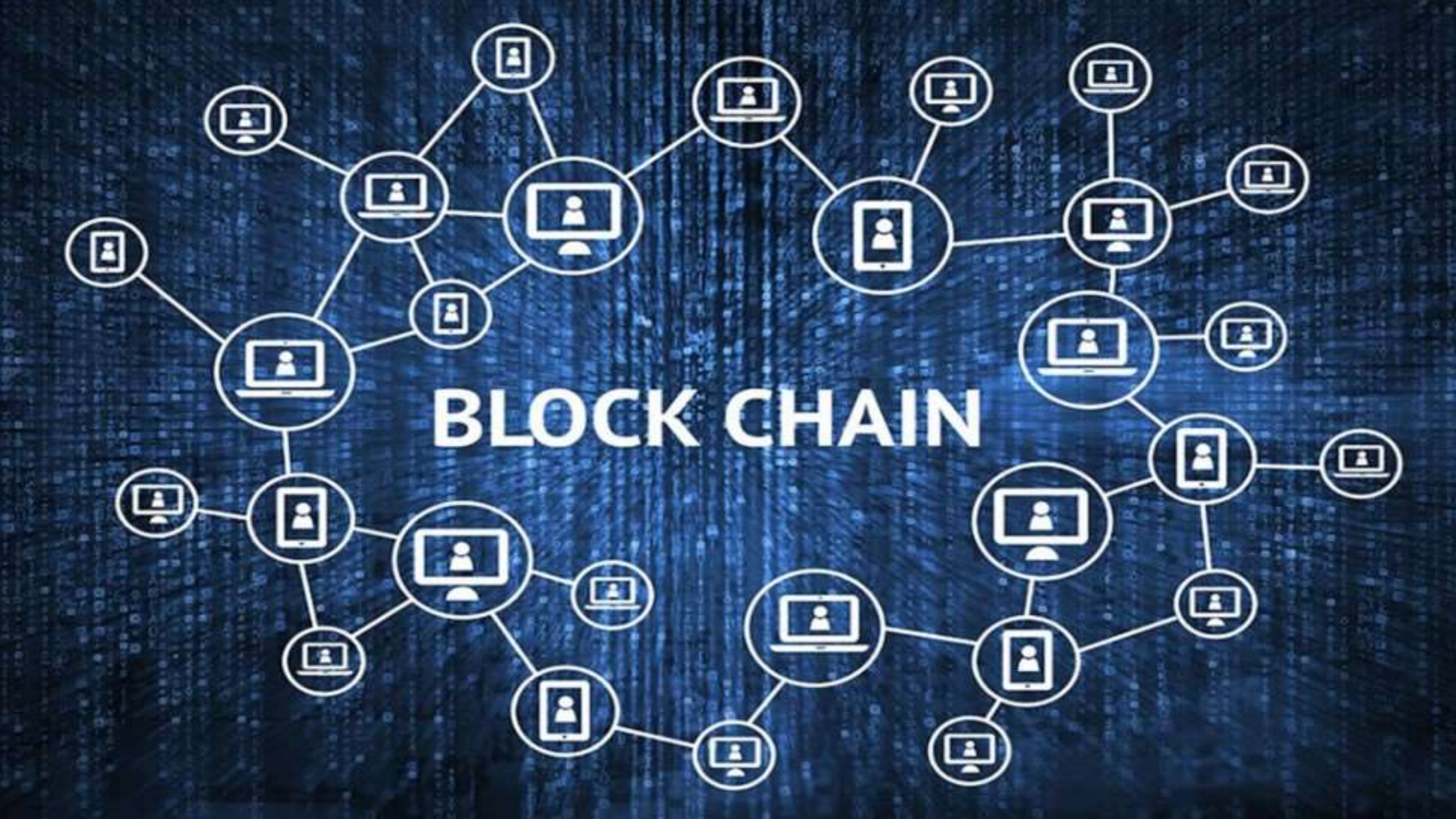
블록체인 Block Chain

소프트웨어와 미래사회

2019


BLOCK CHAIN

[기존 시장생태계에 혁신적인 플랫폼 블록체인]

네트워크 참여자들 간의 신뢰할 수 있는 거래. 탈집중화. 수평적 디지털 비즈니스.

- 2025년 전세계 총생산의 10%가 블록체인 기술로 저장될 것 – 세계경제포럼(WEF)
- 블록체인 시장은 미국이 전체 지출의 40%를 차지하며, 그 다음 서유럽, 중국, 아시아 지역순 2021년에는 4배까지 성장할 것 – IDC 보고서
- 2017년 201억원의 시장규모의 블록체인 시장이 2022년에는 10배 이상 성장할 것으로 전망 - 한국과학 기술원

세계 주요국은 기록보존, 가치전송, 스마트 계약 등 업무 혁신을 가져올 블록체인 도입 본격 추진

- 영국, 에스토니아, 두바이 등 - 선거, 토지 거래 전자문서 유통 등에 도입하기 위한 기술적 검증과 파일럿 구축 등을 선도
- 영국 - 범정부 차원의 블록체인의 효과성을 평가, 지방정부의 실증사업 지원 및 관련 규제 로드맵 발표
- 미국 – 일부 서비스에 도입 중인 블록체인에 대한 법제도적 이슈를 해결하고 실질적 운영을 지원하기 위한 법률 제정 추진 중

거래 속도 지연 및 채굴에 필요한 거래비용 증가

- 미국 내 블록체인 프로젝트 대부분이 중단될 것. 그 중 90%는 실현되지 않을 것 – 포레스터 리서치
- 암호화폐공개(IOC)에 성공한 블록체인 프로젝트이 90%이상이 실패할 것 – 코인원 리서치

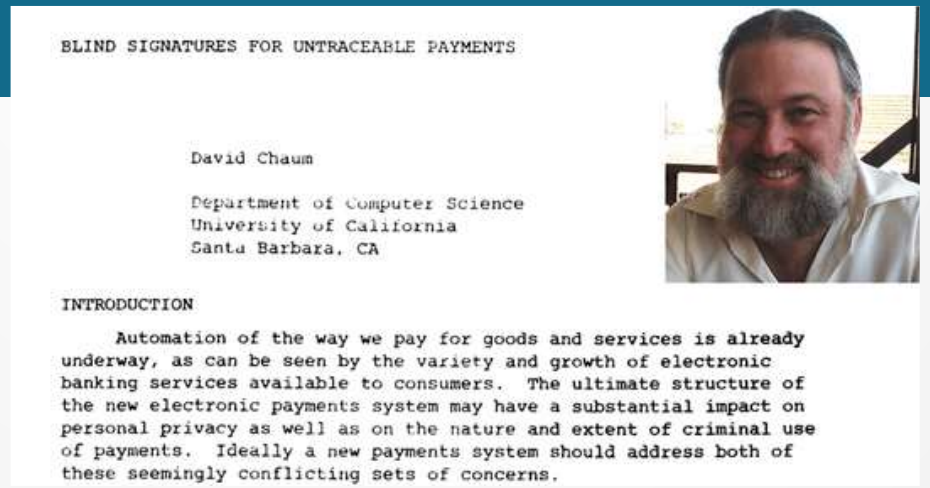
[암호화폐, 가상화폐]

기존 금융거래

- 은행이라는 중앙관리 조직에서 거래 장부 관리
- 2007년 글로벌 금융위기 사태와 같이 중앙집권화의 위험성 존재

암호화폐의 제안

- “Blind Signatures for Untraceable Payments” 논문을 통해
  온라인 상에서 현금처럼 사용할 수 있는 추적이 불가능한 암호화폐 최초 제안
  David Chaum (1982)



BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

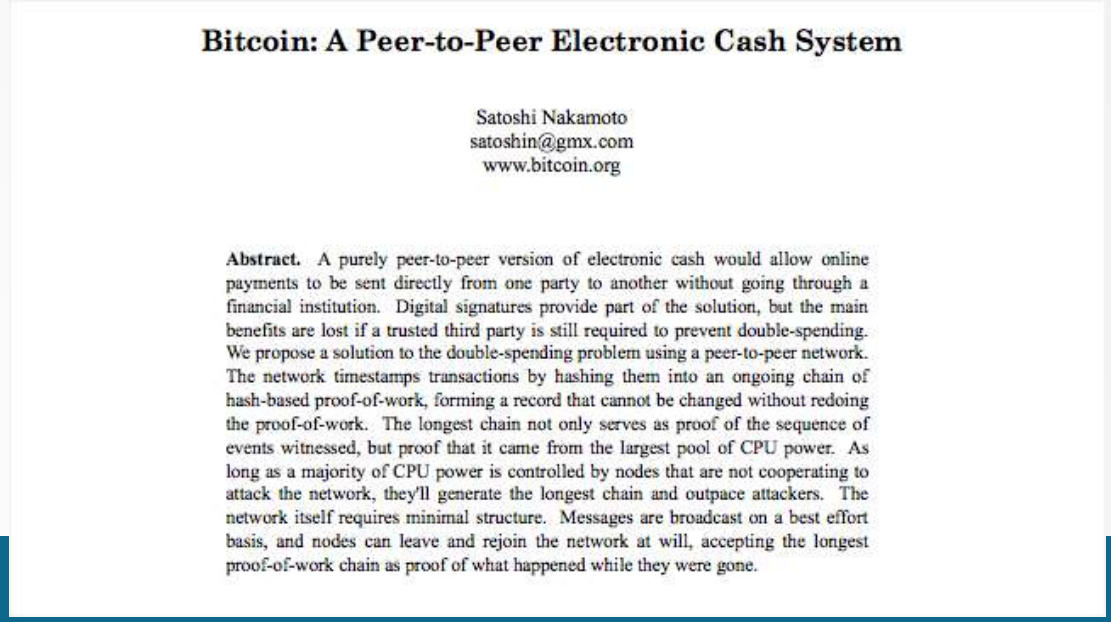
David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

[비트코인의 핵심기술 '블록체인']



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin

- 논문 "비트코인:P2P 전자화폐 시스템" – 사토시 나카모토 (2008.10)
  - "전적으로 거래 당사자 사이에서만 오가는 전자화폐"
  - "P2P네트워크를 활용하여 이중 지불을 막는다"라고 설명 → 블록체인 기술

비트코인은 블록체인 기술을 금융 분야에 적용한 사례

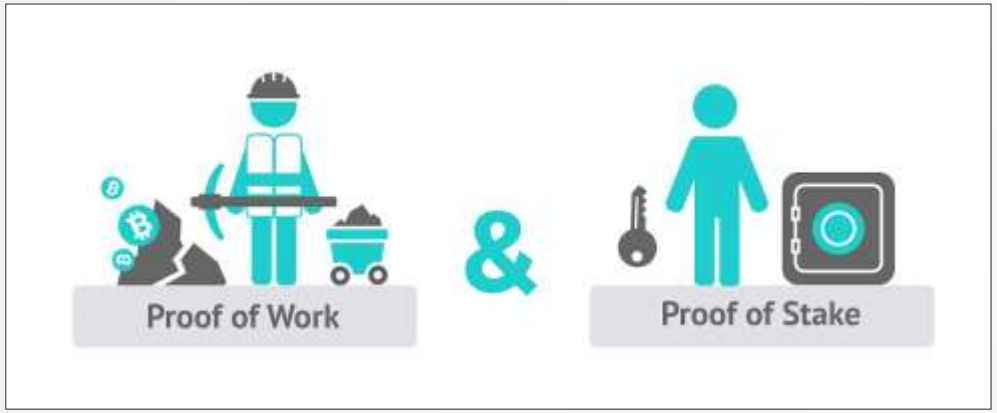
[2세대 블록체인 Ethereum]

- 2015년 출시 : 비탈릭 부테린(Vitalik Buterin)
- 내장 프로그래밍 언어 '솔리디티(Solidity) '
- 2013년 '차세대 스마트 계약 & 분산 응용 애플리케이션 플랫폼' 발표
- 금융거래에 한정, 특화된 기존 블록체인 시스템을 금융거래 이외의 모든 분야로 확장

- Smart Contract

  - 코드에 적힌 계약 조건이 만족되면 그 즉시 계약 성립

  - 차세대 스마트 계약 : 각 비즈니스 로직에 따른 복잡하고 다양한 계약 패턴 소화



<이미지 출처: Perfectial 블로그>

- 이더리움은 작업증명에서 지분증명으로 전환중
- 화폐를 더 많이 소유한 참가자가 우선적으로 블록을 생성(자원 소비 감소)

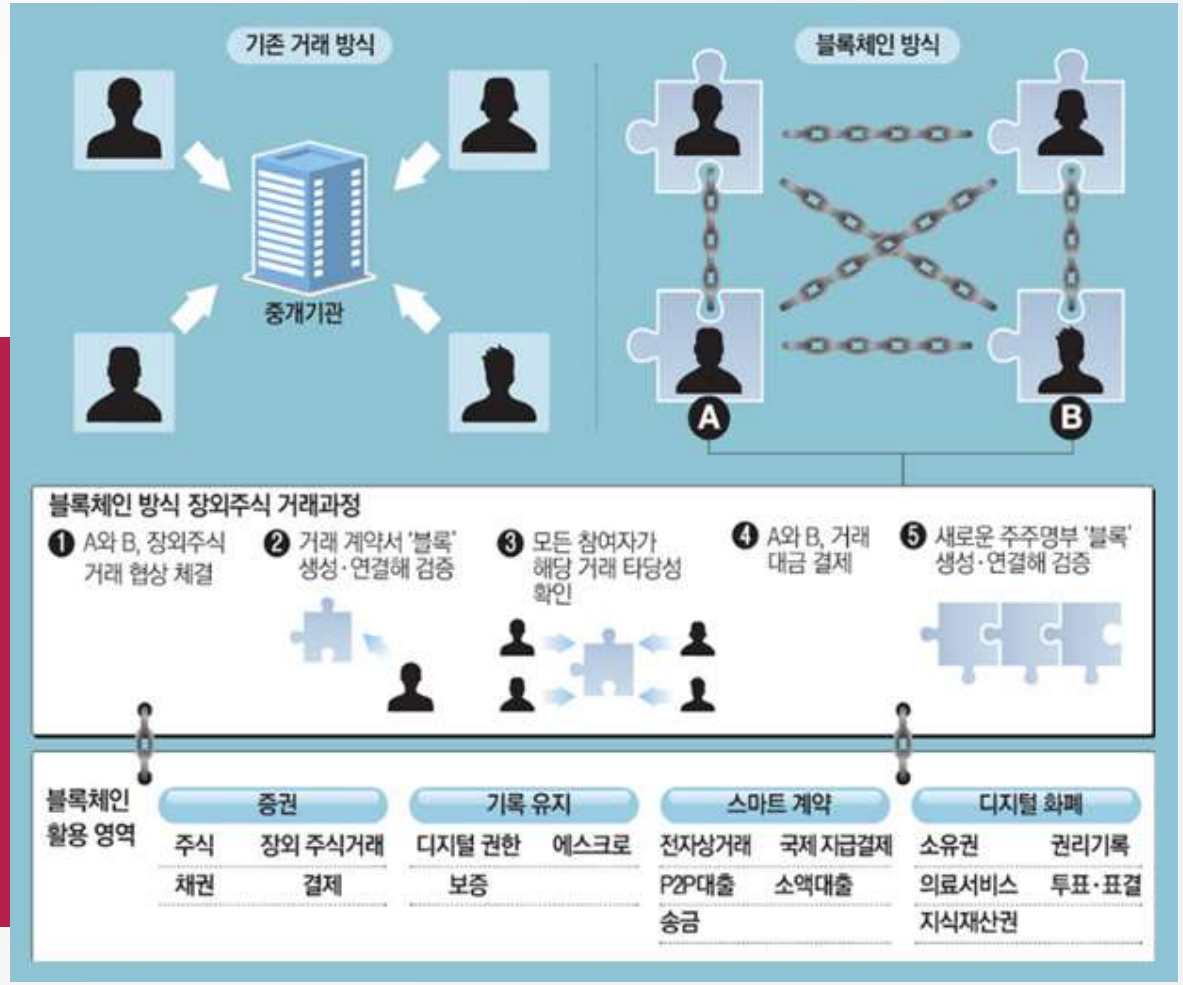
[블록체인이란?]

P2P 프로토콜 기반의 분산 원장 기술 (DLT : Distributed Ledger Technology)

블록(block) + 체인(chain)

- 블록 : 개인과 개인간의 거래 (P2P) 데이터가 기록된 장부
- 블록들이 일정 시간 흐름에 따라 순차적으로 연결되는 사슬 구조
- 중앙기관 또는 제3자의 개입 없이 신뢰할 수 있는 거래 가능

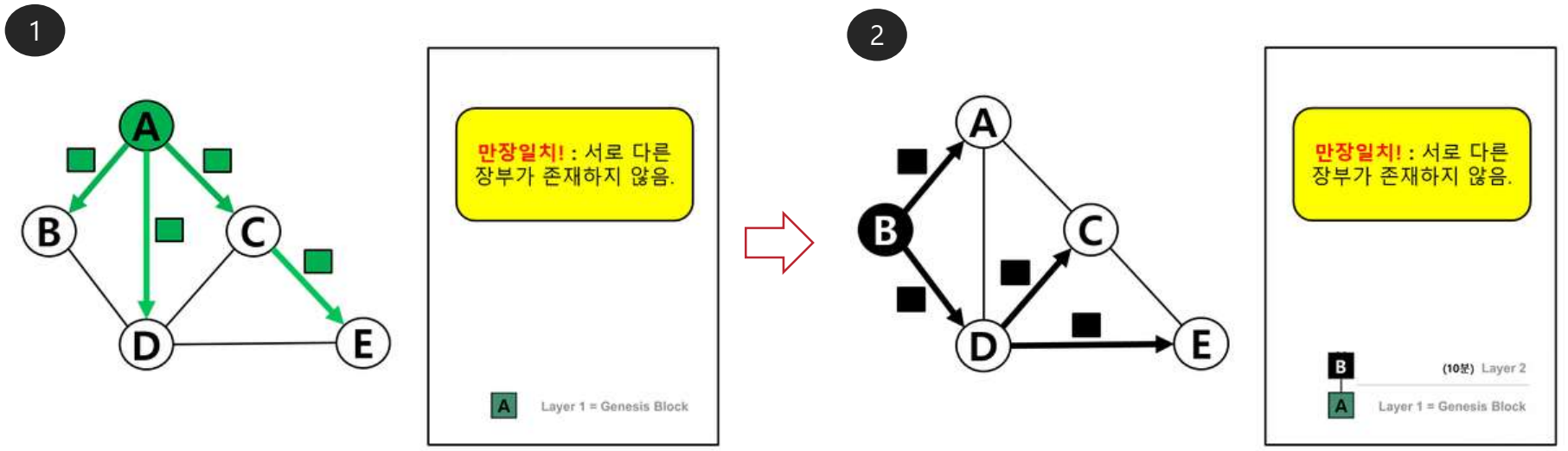
- 분산되어 있고
- 증명가능한 방식으로 서명되고
- 추가만 가능하며
- 순차적으로 연결되고
- 암호학적으로 안전하게 복제되는
- 소프트웨어 주도 합의체계



[블록체인의 진행원리]

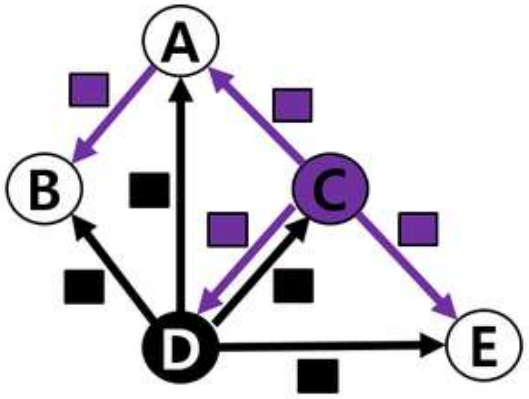
1. 거래 데이터를 10분에 1회씩 모아 거래내역 묶음인 블록을 만든다
2. 만들어진 블록은 블록체인 네트워크내 모든 참여자에게 보내진다
3. 참여자에 의해 타당한 거래에 대한 검증 및 승인이 이루어진다
4. 검증 및 승인이 완료되면 기존 블록체인에 연결된다
5. 한번 연결된 블록체인은 영구히 저장된다

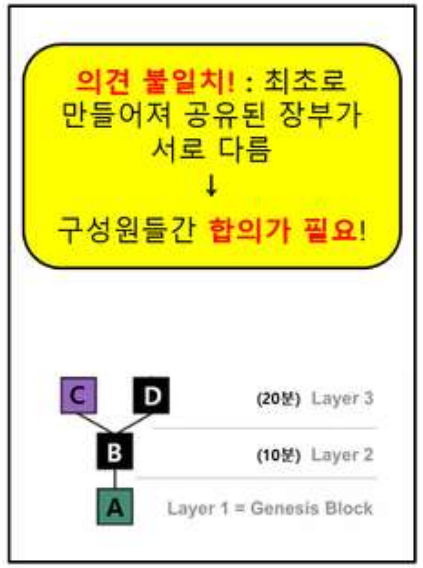
   (한번 연결된 거래기록은 수정이 불가능하며, 위 과정이 반복되어 블록체인 형성)



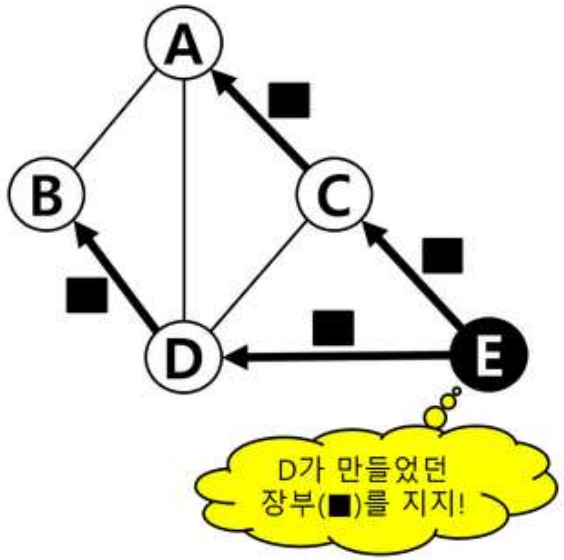
[블록체인의 진행원리]

3

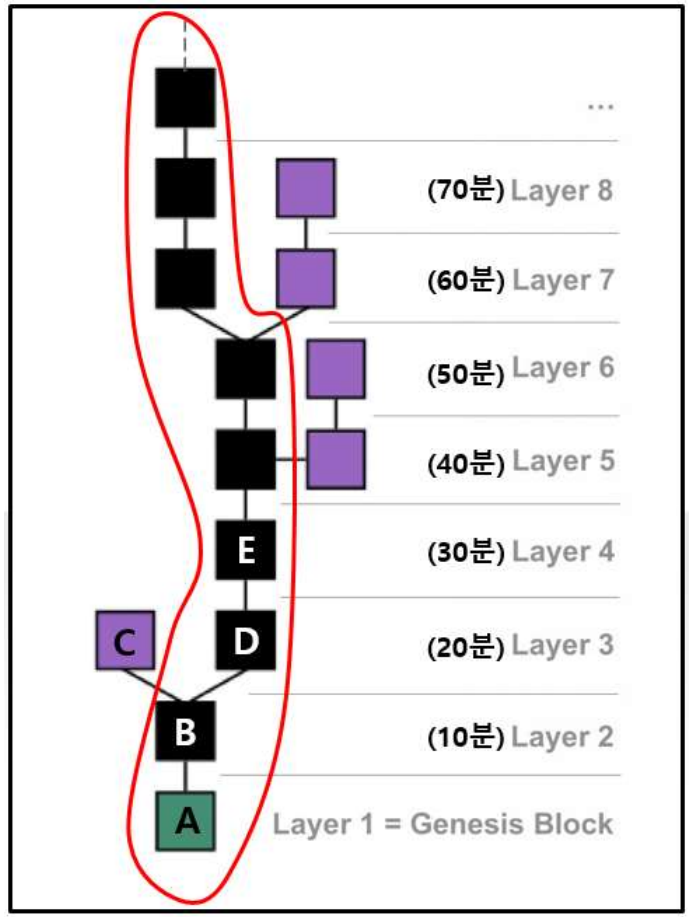




4



5

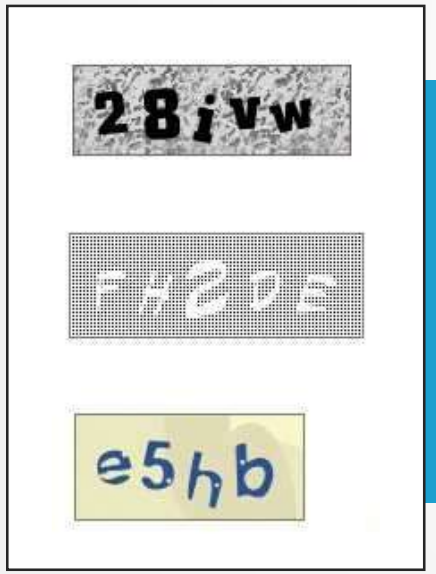


블록체인의 동작 과정 (출처:https://amhoin.blog.me)

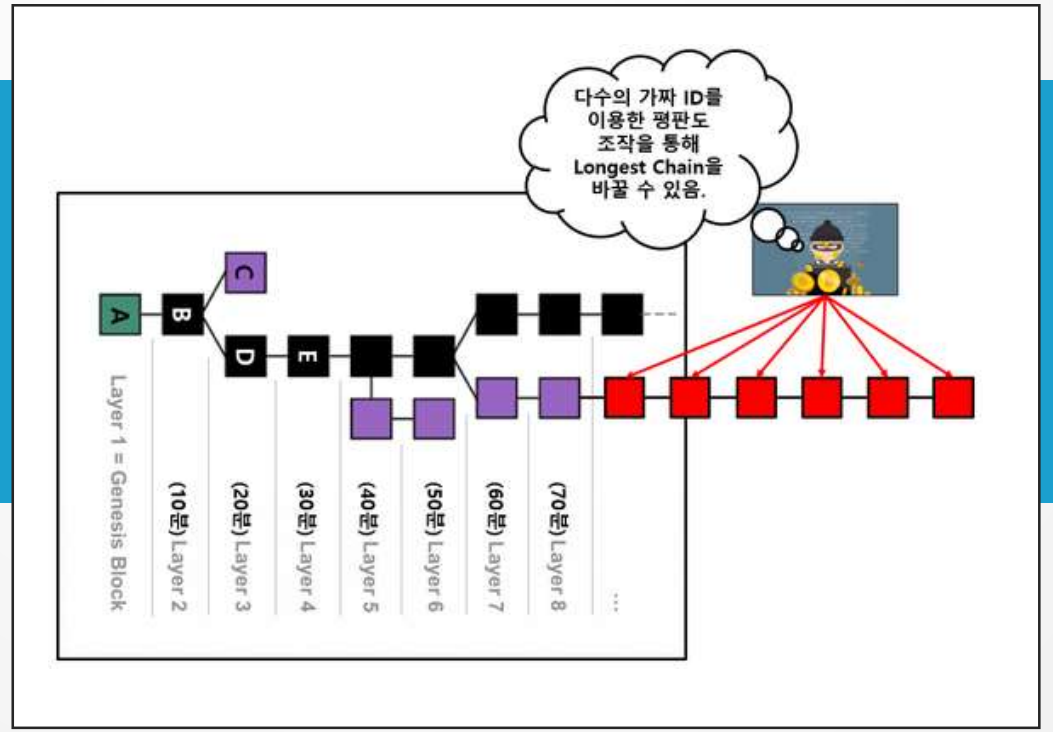
[블록체인 작업 증명 Proof of Work]

- 인터넷상에서 자발적 합의(Consensus)를 이루는 것은 상당히 어려움
- 불순한 의도를 가진 사용자가 허위로 여러 개의 ID를 만들어 틀린 블록을 옳다고 할 경우 제대로 된 감시가 어려움
- 사용자들이 블록을 만들어 공유하고자 할때마다 캡챠(Captcha)와 같은 복잡한 암호 퍼즐을 풀도록 설계

  - 작업 증명 proof of work



[captcha]



[Sybil Attacks]

(출처:https://amhoin.blog.me)

[비트코인 채굴?!]

- 검증과정에 참여하는 컴퓨터를 채굴자 (miner)라고 부름
- 수많은 컴퓨터 들 중 한 컴퓨터가 새롭게 검증된 거래내역 파일을 성공적으로 덧붙이면 그 컴퓨터에게 상으로 비트코인이 주어짐
- 많은 컴퓨터로 네트워크에 참여하면 비트코인을 얻게 될 확률이 높아짐 → 불순한 의도를 막기 위해 작업 증명 요구
- 이중지불 수법이 비트코인에서 불가능한 것은 아니지만 엄청난 비용 소모

  - 51% 공격을 하기 위해 추산되는 장비와 전기요금은 약 22억 달러(2조 4천억원)

[전문채굴꾼]

암호화폐와 블록체인의 문제점

- 합의에 의한 탈중앙화 → 확장성 문제 야기
- 여론조작을 막기위한 작업 증명 등의 기술 → 과다한 전력 소모문제 발생
- 삭제의 어려움 → 개인 사생활 침해
- 다른 사람의 PC를 이용해 모래 비트코인을 채굴하는 봇넷(botnet) 등장
- 불완전한 익명성, 보안이 취약한 오픈소스

[블록체인의 유형 및 특성]

Public (참여형)

- 누구나 참여 가능 : Bitcoin, Ethereum
- 익명성
- 동의 (Consensus) 프로토콜 : POW (Proof of work) ➔ 성능, 비용, 확장성 제약

Private/Consortium (허가형)

- 허가받은 멤버만 참여 가능
- 실명제
- 동의 (Consensus) 프로토콜 : 멤버의 선택 (PBFT, No-Op 등) ➔ 높은 확장성과 성능

블록체인의 4가지 특성

- 공유와 투명성, 불변(Immutable), 검증 및 부인 방지, 기밀성을 위한 암호화

[블록체인의 활용]

복잡한 거래를 단순하게 만드는 블록체인

물류

- 실시간 가시성
- 개선된 효율성
- 투명성 및 검증
- 감소된 비용

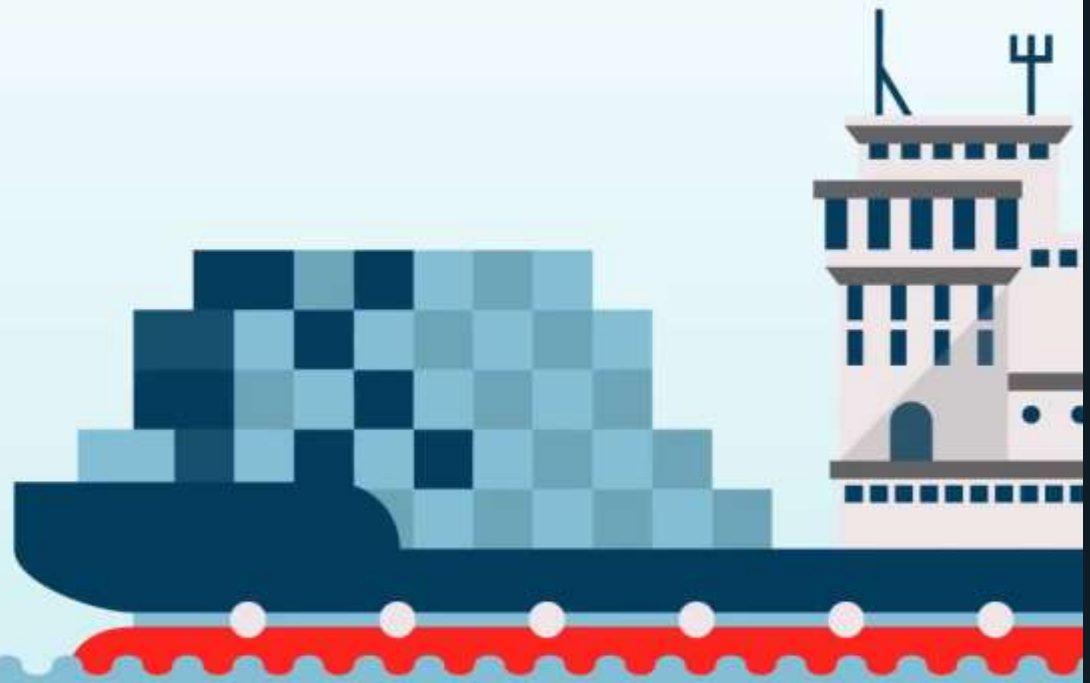
부동산

- 위조 불가능
- 더욱 줄어든 분쟁
- 투명성 및 검증
- 낮은 전달 수수료

금융

- 빠른 정착 시간
- 증가된 신용 이용성
- 투명성 및 검증
- 조정 비용 없음

SK 주식회사
C&C



블록체인 기반 국제 물류 네트워크 서비스 SK 주식회사

[국내 블록체인 도입 사례]

- 전기화재 발화지점 분석 지원 (SK텔레콤)
  - 전기 화재 발화의 80%를 차지하는 스파크 발생정보를 블록체인에 보관
- 실손의료보험금 자동 청구 (교보생명)
  - 보험가입자의 진료기록을 블록체인에 기록하여 병원과 보험사가 실시간 공유
- 이웃간 전력거래 (한국전력)
  - 블록체인 기반 전력거래 플랫폼 통해 최적의 전기 생산자와 소비자 매칭
- 해운물류 실시간 정보 공유 (삼성SDS)
  - 송·수화자, 운송사, 항만청 등이 물류운송관련정보를 블록체인을 통해 실시간 공유
- 의료 데이터 상호운용 (메디블록)
  - 불필요한 중복검사를 막기위한 블록체인 기반 의료 정보 공유 플랫폼

(자료 : 과학기술정보통신부)

[해외 블록체인 사례]

- 중국 항저우 2025년 완공을 목표로 블록체인기반 스마트시티 구축
  - 지갑과 종이가 없는 페이퍼리스 공공금융거래, 친환경 에너지 개인간 거래. 호구(주민등록) 관리 등
- 두바이 '글로벌 블록체인 의회(Global Blockchain Council) 설립 2016.02
  - 블록체인 추진전략 발표 : 환자 이력 관리, 관광객 편의 시스템 구축

- 자전거를 블록체인 플랫폼으로 관리 – 네덜란드 차장 등록청
- 블록체인으로 개인 간 전력 판매를 허용하는 프로그램 시작
  – 호주 에너지분야 신생업체 파워레저(Power Ledger)

- 블록체인을 활용하여 예술작품, 원고, 사진 및 이미지 원본 작품을 분류하고 저장하는 시도
  - Blockai, TinEye, Mediachain 등

- IBM-머스크 물류 블록체인 등

(자료 : 과학기술정보통신부)

[암호화폐의 위기 ?!]

- 전세계 암호화폐의 종류는 1000여개 이상. 전체 시가 총액 2000억 달러 (약 225조원)
- 암호화폐 급락 << 확장성의 문제. 보안 취약성.
- 암호화폐 시장을 잡기위한 국가, 기업의 노력 계속

확장성은 암호화폐 이해관계자 간 득과 실 차이로 쉽게 합의하기 어려운 문제입니다.

한쪽에서는 네트워크 효율을 높이기 위해 블록 크기를 키우려 하고,

다른 쪽에서는 블록체인의 핵심 기조인 탈중앙화를 고수하는 데 힘쓰죠.

탈중앙화를 유지한 채 효율을 끌어올리는 데 한계가 있기 때문에 두 진영은 끊임없이 충돌합니다.

갈등을 해결하려면 둘 사이에서 균형점을 찾는 게 중요합니다

– 미국 노스웨스턴 대학 켈로그 경영대학원 교수 새릿 마코비치(Sarit Markovich)

[블록체인 활용에 따른 과제]

P2P 네트워크 문제	네트워크 단절과 공격
	노드 신뢰성 및 전달의 확실성
	전송횟수와 지연 등의 성능
합의 알고리즘 문제	Finality 불확실성
	악의적 참가자 (51% 문제)
	실시간 업무 처리
보안 문제	기밀성 문제
	계정의 정당성 및 개인정보

대응 방안

- 허가형 네트워크
- 합의 알고리즘 선택
- 블록 정보의 암호화
- 트랜잭션마다 인증변경

[출처 : 블록체인 구조와 이론]

THANK YOU
FOR LISTENING!